



Ingeniería en Informática

Sistema de control de acceso a aplicaciones web con autenticación biométrica

Walter Gabriel Ortiz Medina

**Tutor:
Roberto Sánchez**

**Línea de Investigación:
Seguridad Informática**

**Asunción – Paraguay
2024**



ÍNDICE

Dedicatoria.....	iii
Tabla de Contenido.....	iv
Tabla de Figuras	viii
Tabla de Abreviaturas.....	ix
Resumen	1
Introducción.....	2
Planteamiento del problema de investigación	2
Preguntas de investigación	3
Objetivo General.....	4
Objetivos Específicos	4
Justificación	4
Alcance y limitaciones del Proyecto	5
Forma de Investigación.	5
Tipo de Investigación.	6
Marco Teórico	6
Antecedentes Internacionales	7
Antecedentes nacionales.....	8
Bases teóricas	8
Control de Acceso	8
Funcionamiento del Control de Acceso	9
Finalidad del Control de Acceso	9
Autenticación.....	9
Autenticación y Seguridad.....	10
Verificación de identidad mediante factores de autenticación	10
Factores de autenticación adicionales.....	11
Autenticadores para dispositivos Android y IOS	11
Google Authenticator	11
Microsoft Authenticator	11
Autenticación biométrica.....	11
Funcionamiento de la autenticación biométrica	11
Ejemplos de autenticación biométrica	12
Herramientas y Tecnologías de autenticación	12



Passkey	12
WebAuth.....	12
Autorización	13
Gestión de la autorización en un sistema informático	13
Navegadores Web.....	13
Gestores de Contraseñas	13
Aspectos legales	14
Tecnologías y proyectos utilizados.	14
Socket.io	14
Prerrequisitos.	14
Funcionamiento general de Socket.IO.....	15
Inicializar el servidor:	15
La Instancia del Socket (Lado del Servidor)	15
Instancia del Servidor (io) de Socket.IO	16
ID del Socket	16
La Instancia del Socket (lado del Cliente).....	16
Electron JS.....	16
Prerrequisitos	16
Android.....	17
Laravel	17
Postgresql	17
Especificación de la solución	18
Arquitectura de la solución.....	19
Componentes de Software	19
Componentes de Hardware:.....	20
Componentes de Infraestructura de Red:.....	20
Autenticación por Grupos.....	21
Arquitectura del Sistema de Administración Web.	21
Partes de la Arquitectura del Contenedor Web:	23
Arquitectura del Autenticador	24
Casos de Uso	24
Casos de uso del Contenedor Web:	24
Casos de uso del Autenticador:	25
Aplicación Web	28



Funcionamiento del Contenedor Web	29
Validaciones en el Contenedor	29
Validaciones en la API	29
Cierre por Inactividad	31
Botones de Navegación.	31
Funcionamiento del Autenticador.	31
Lector de Huellas.....	33
Características del Autenticador	34
Servidor de Socket.Io	34
Proceso de Asignación de Huella Dactilar	36
Configuración de Autenticadores y Contenedores.	38
Proceso de Gestión de Credenciales Web	39
Inserción automática de Credenciales	40
Método 1.....	40
Método 2.....	41
Configuración de una Página Web	43
Base de Datos	43
Herramientas Utilizadas	45
Requerimientos funcionales	45
Requerimientos No Funcionales.....	45
Requerimientos mínimos de Software.....	45
Contenedores:	45
Autenticadores	46
Aplicación Web	46
Web Server	46
Base de Datos	46
Requerimientos mínimos de Hardware	46
Contenedores:	46
Autenticadores	46
Aplicación Web y Socket	46
Base de Datos	46
Componentes de Infraestructura de Red.....	47
Contenedores:	47
Autenticadores	47



Servidor Web y Socket	47
Base de Datos	47
Prueba y resultados	47
Aplicación RRHH	48
Aplicación Ventas.....	49
Conclusiones y recomendaciones	49
Investigaciones Futuras	50
Referencias	50



RESUMEN

El uso de aplicaciones web plantea desafíos en términos de seguridad de datos, especialmente en organizaciones como los Contact Centers donde el número de usuarios concurrentes suele ser elevado, en estos entornos se presentan escenarios que podrían poner en riesgo la confidencialidad de la información debido principalmente al robo de credenciales. Este trabajo de investigación tiene como objetivo desarrollar e implementar un sistema de control de acceso y navegación a aplicaciones web, eliminando la necesidad de recordar las credenciales de acceso a dichas aplicaciones, ya que el sistema cuenta con un gestor de contraseñas integrado que se encarga de descifrar e introducir automáticamente dichos datos en las aplicaciones web. Para realizar este proceso el usuario primero se autentica en el sistema con su nombre de usuario y verifica su identidad mediante un dispositivo autenticador común utilizando su huella dactilar. La administración del sistema se realiza a través de una plataforma web y permite gestionar las diferentes entidades del sistema, como los usuarios, sus huellas, grupos, y las aplicaciones web. Uno de los beneficios de implementar la solución es que las aplicaciones web a las que accede el usuario no requieren de ningún tipo de implementación adicional, más que ser compatibles con la plataforma de navegación. Finalmente, con todas las pruebas realizadas se concluye que la plataforma funciona fluidamente permitiendo al usuario acceder de manera segura a las aplicaciones web desde una estación de trabajo utilizando un nombre de usuario y validando su identidad mediante el uso de un autenticador biométrico.

Palabras clave: autenticación biométrica, gestión de credenciales, contact centers.